**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 294**

Security Equipment

**Security Software**

Describe each of the following software-based security types.

1. Encryption software
   1. What are the two types of modern encryption methods?  
      symmetric-key encryption and Asymmetric-key encryption.
2. Network policies, profiles  
   many organisations now use networks to enable employees to access data stored in different locations. In some cases, staff members may be located in different parts of the world, but working together on a single document. To enable employees to gain access to some files, but restrict them from others, a network administrator will establish a series of network policies and profiles
3. Firewalls  
   Firewalls are another type of network protection, used to restrict access by outsiders to a network, as well as to protect confidential information, such as payrolls and personnel records, from employees not authorised to access it.
4. Antivirus software  
   Antivirus software can be used to prevent computer virus infections. This software detects the presence of viruses as the computer boots up, when an executable file is run, when documents are accessed or when files are copied. Antivirus programs will also detect viruses in files downloaded from the Internet.

**Security Procedures, p 299**

**Communication:**

1. List the security considerations for communication within an organisation.  
   - Well-documented processes for communication sensitive information via email, telephone and fax.  
   - Use of passwords on documents that have sensitive information.  
   - Well-documented policy for the use of networked devices within the organisation.

**Storage**

1. **File naming conventions**
   1. List the 3 types of information each document should include.  
      - **Date stamp:** A date that indicates the timeliness of a document. This information is different from the metadata saved with each file that indicates when the document was created and when it was last saved.  
      - **Variation:** identifying which version of the file is saved for example, track of which version they are working on.  
      - **Name:** Something meaningful that can identify the document.
   2. Give an example of a sequential file-naming convention.  
      ‘Newsletter 2011-11 03Oct.doc’. This is a monthly newsletter. The edition being prepared is for the November 2011. The revision was saved on 3Oct and is named sequentially.
2. **Location of files**where you store yours files is just as important as what you call them.
3. **Backups**
   1. Distinguish between each of the following:
      1. Full backup  
         copies all of the files from a device to a storage medium. Takes considerable time and is usually performed once over a time period (week, fortnight, month).
      2. Differential backup  
         Copies of data would involve restoring files from the full backup and then from the differential backup.
      3. Incremental backup  
         Similar to differential backup, the difference being that is uses more than two backup media, while a differential backup only uses two media.
4. **Backup timeline**
   1. List good practice in relation to backup timelines.  
      It is a good practice to clearly label all backup media so that you know when the backup was made and what is on it. A log may also be kept by a systems manager recording backup dates, the location of backup files and whether any restorations have been made.
5. **Location of backup files**
   1. List good practice in the relation to the storage of backup files.  
      Have multiple copies of backups on onsite and/or offsite, in case one gets destroyed and so you have multiple copies of data.
   2. What is the grandparent-parent-child system?  
      The parent is the second oldest copy of this file. The child is the most recent copy of the file. And incremental backup is performed each day, with a differential backup at the end of each week. A full backup is done at the end of each month.
6. **Archiving and destruction**
   1. Distinguish between archiving and destruction?  
      Archiving is essentially a process of copying files to a long-term storage, then deleting hem from the hard disk.  
      Destruction involves deletion only.
   2. What is a problem for ICT managers?  
      Determining which the most appropriate long-term storage medium to use is.
   3. What is a legacy system?  
      An old system is generally referred to as a legacy system. These systems might run old databases on old servers or mainframes.
7. **Disposal**
   1. What issues must organisations consider in disposing information?

Disposal of old equipment also poses a challenge for organisations, as companies sometimes do not consider issues of protecting sensitive data when disposing of old computer equipment. There are currently many ways of ‘deleting’ data from a storage medium, but none of these techniques can completely guarantee that your information is properly disposed of.